ESXI 6.5 Configuration Guide

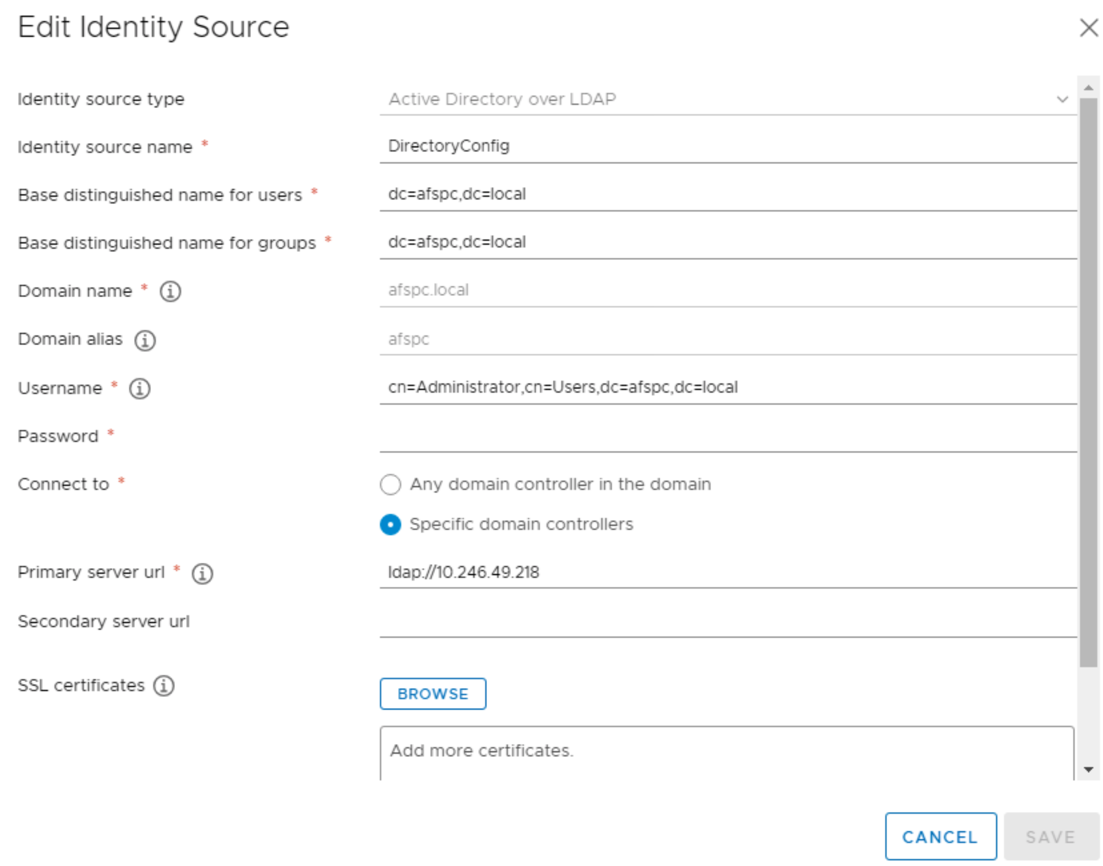
This document is designed to be used in conjunction with a PUA implementation.

N.B. It should be noted that this configuration relies on creating a separate VIP and access policy for ESXI and using “Multiple Domain Based SSO” with the login page for this VIP being the main PUA webtop access VIP. Then an “external webtop Item” is created and hosted on the webtop. Also there is an accompanying iRule that injects java script into the login page to force the login. Also note that this configuration is for the HTML5 client for ESXI.

1) Configure Directory Services for Esx

   Log into ESXI with Local User

   Select “Administration/Configuration”
   And “Identity Sources”



Edit Identity Source

Identity source type	Active Directory over LDAP
Identity source name *	DirectoryConfig
Base distinguished name for users *	dc=afspc,dc=local
Base distinguished name for groups *	dc=afspc,dc=local
Domain name *	afspc.local
Domain alias	afspc
Username *	cn=Administrator,cn=Users,dc=afspc,dc=local
Password *	
Connect to *	○ Any domain controller in the domain ● Specific domain controllers
Primary server url *	ldap://10.246.49.218
Secondary server url	
SSL certificates	BROWSE Add more certificates.

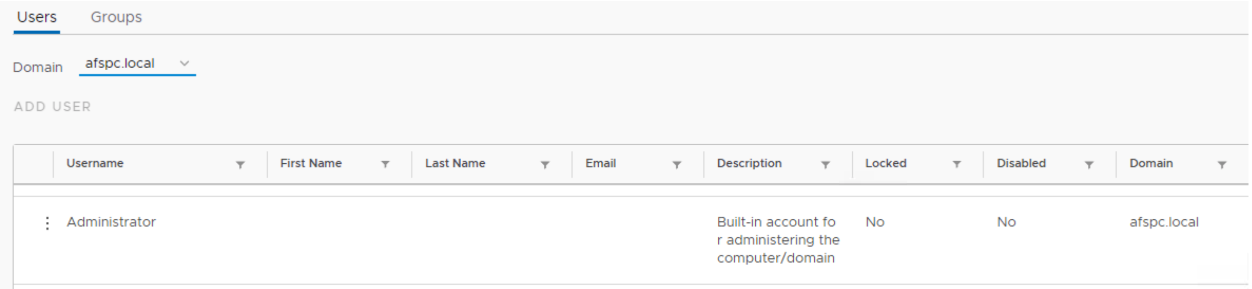
   Select “Add Identity Source”

   - For Identity Source Type Select “Active Directory over LDAP”

- Provide a Name
- Configure the Base Distinquished Name for Users for example:- dc=afspc,dc=local
- Configure the Base Distinquished Name for Groups for example:- dc=afpsc,dc=local
- Domain Name:- For example afspc.local
- Domain Alias:- afpsc
- Username for example:- cn=Administrator, cn=Users, dc=afspc, dc=local
- LDAP Server: < THEIPADDRESSOFYOURPUAVIPFORLDAP >
- Password: The Password of the User that will connect to the Directory Server
- Under Connect to: ldap://<THEIPADDRESSOFYOURPUAVIPFORLDAP>
    - According to the ESX documentation if you do not specify a port then it will default to 389.
- If using ldaps this will be ldap://< THEIPADDRESSOFYOURPUAVIPFORLDAP >:636
- Also if using ldaps certificates may need to be uploaded
- Select the “Add Button” if there is a configuration issue then the “Add will fail”

Under Users and Groups
Select Your Domain for example “afpsc.local”

You should then be able to see Active Directory Users and Groups Populated in the User Interface.

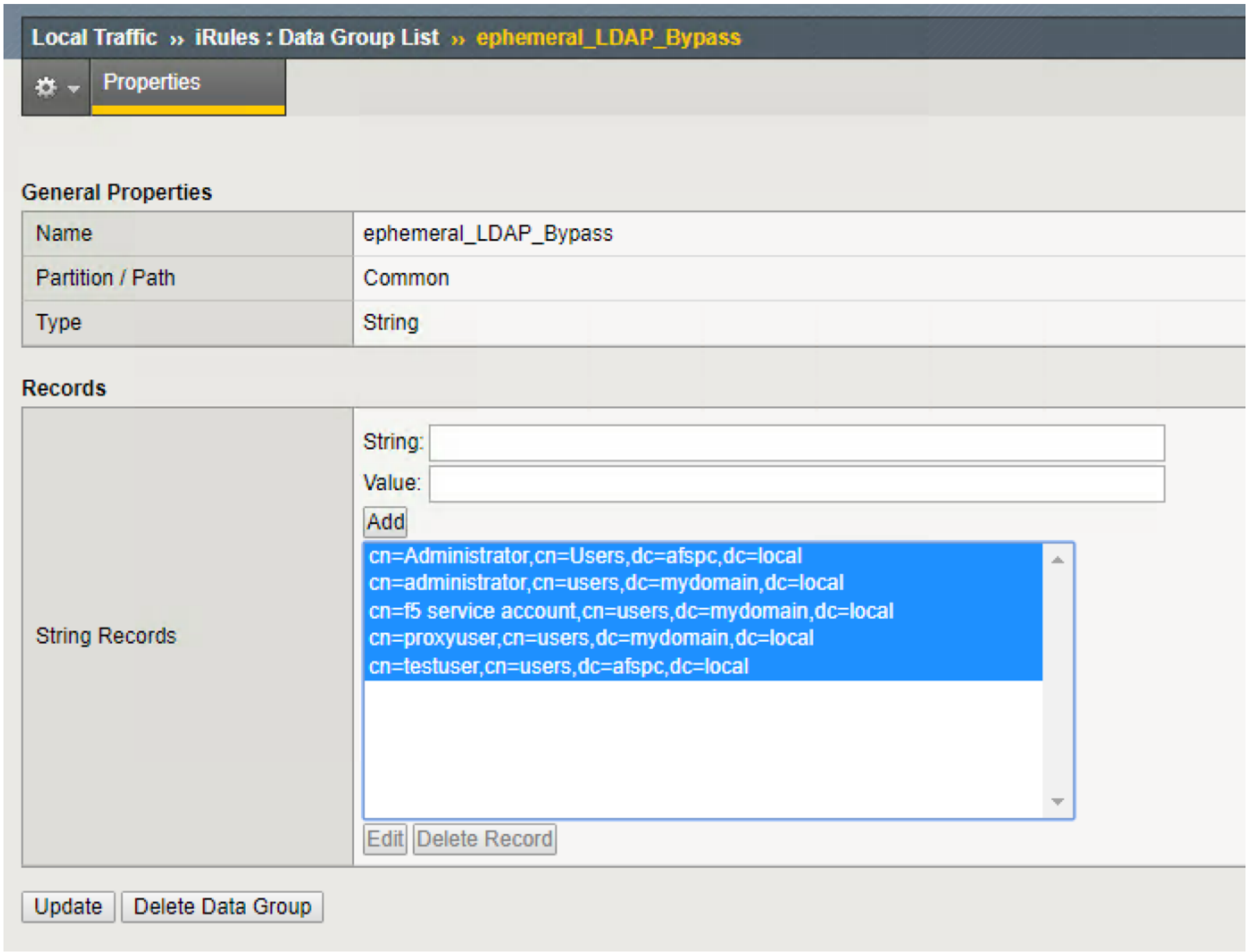


	Username	First Name	Last Name	Email	Description	Locked	Disabled	Domain
⋮	Administrator				Built-in account for administering the computer/domain	No	No	afspc.local

.

Logout of theESXI Server.. and then Log Back in with an Active Directory User to verify that you can login to the system with an AD User directly the Unity User Interface (no Big-IP)

Note: The DN that username translates to must be in the ephemeral_LDAP_Bypass data-group. Otherwise the PUA system will intercept the authentication and generate an ephemeral credential and the authentication will fail. This data group is under iRules/DataGroup List


Local Traffic » iRules : Data Group List » ephemeral_LDAP_Bypass
Properties

General Properties

Name	ephemeral_LDAP_Bypass
Partition / Path	Common
Type	String

Records

String Records

String:
Value:

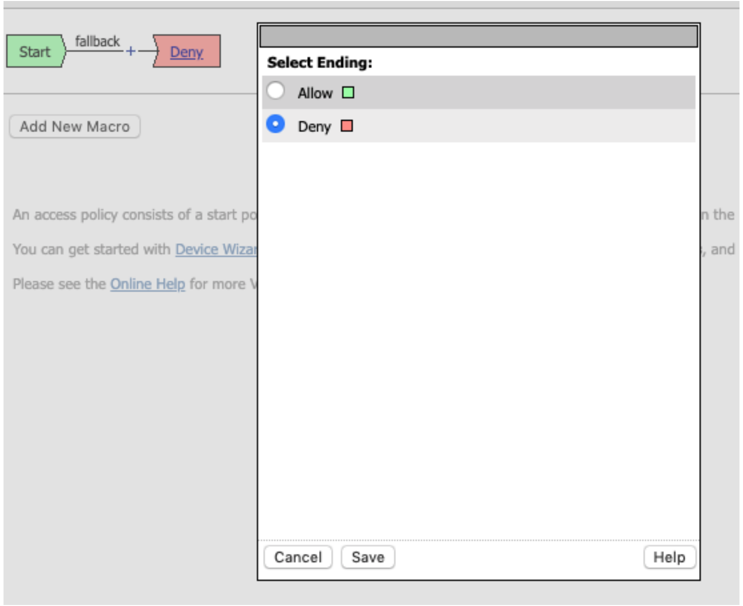
```
cn=Administrator,cn=Users,dc=afspc,dc=local
cn=administrator,cn=users,dc=mydomain,dc=local
cn=f5 service account,cn=users,dc=mydomain,dc=local
cn=proxyuser,cn=users,dc=mydomain,dc=local
cn=testuser,cn=users,dc=afspc,dc=local
```

Edit
Delete Record
Update
Delete Data Group

2) Create Access Policy for ESXI

Under Access/ “Profiles/Policies”/Access Profiles (Per Session Policies) click “create”.

Provide a name for your access Policy for example:- “ESXI”
For Profile Type Select:- LTM+APM
For Profile Scope Select:- Global
Under Accepted Languages Select:- English
Select Finished.
Under Per Session Policy Select “Edit”
Change the ending to “Allow”.. by clicking on the “Deny” ending and then select the radio button for “Allow”


Start
fallback
Deny
Add New Macro
An access policy consists of a start po
n the
You can get started with Device Wiza
, and
Please see the Online Help for more
Cancel
Save
Help

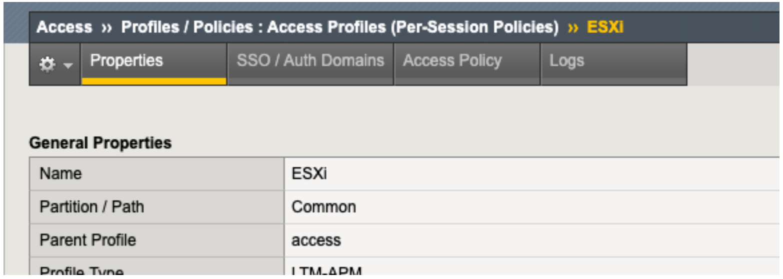
Select Ending:

○ Allow 🟩

● Deny 🟥

Associate the SSO/Auth Domain with the Access Policy

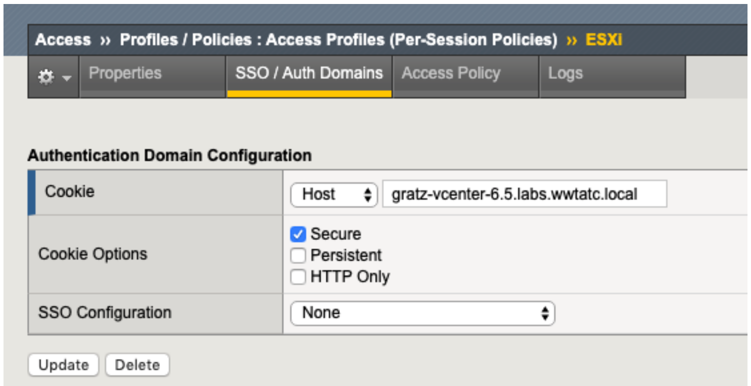
- Under Access/Profiles/Policies click on the Access Profile Name ..for instance click on “ESXI” if your access profile is called ESXI.
- The properties will be displayed..
- At the top click on the SSO/Auth Domains TAB.


Access » Profiles / Policies : Access Profiles (Per-Session Policies) » ESXi
Properties
SSO / Auth Domains
Access Policy
Logs

General Properties

Name	ESXi
Partition / Path	Common
Parent Profile	access
Profile Type	LTM-APM

- For Domain Mode select “Multiple Domains:
- For primary Authentication URI.. this will be the FQDN for your PUA webtop for instance : https://pua.lab.com
- Under Authentication Domains Select : “Add”
- Then under “Cookie” select “Host”
- For DNS name select the FQDN of the ESXi VIP.
- Make the Cookie “Secure”
- For SSO Configuration select “None”



Access » Profiles / Policies : Access Profiles (Per-Session Policies) » ESXi

Authentication Domain Configuration

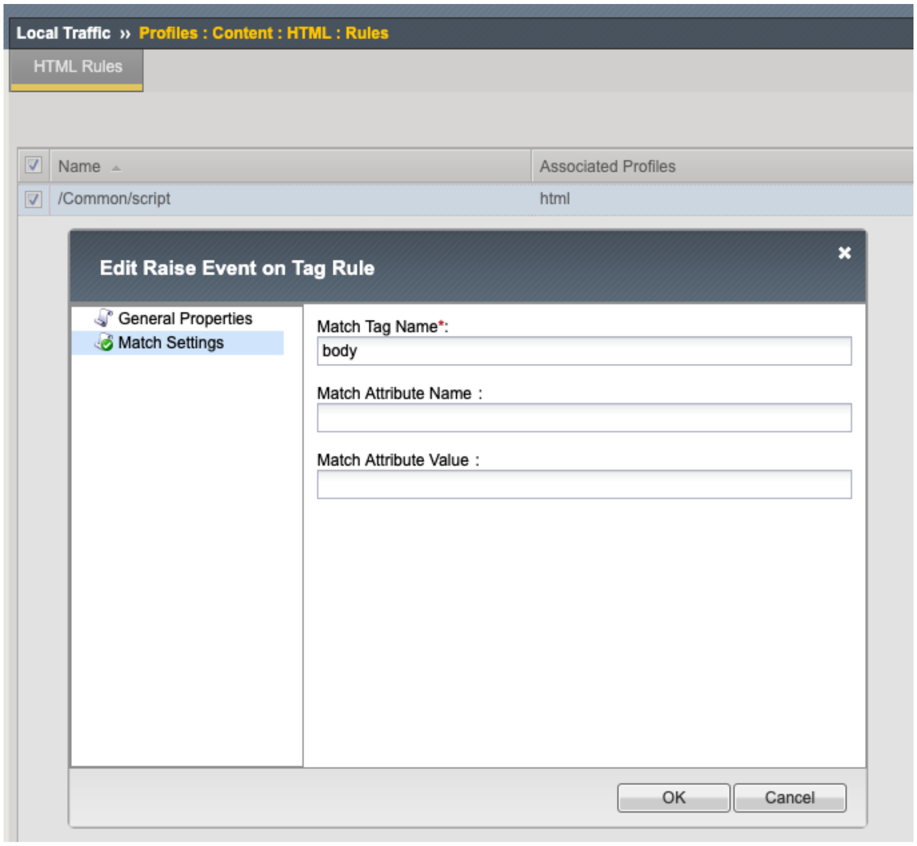
Cookie	Host gratz-vcenter-6.5.labs.wwtatc.local
Cookie Options	☑ Secure ☐ Persistent ☐ HTTP Only
SSO Configuration	None

3) Create an HTML content profile rule

This profile will be used in conjunction with the iRule for SSO for ESXI.

Under Local Traffic/Profiles/Content/HTML/Rules

Select “Create New”
Provide a name:- “Script”
Under “Match Settings” for Match Tag Name type:- body



Local Traffic » Profiles : Content : HTML : Rules

☑	Name	Associated Profiles
☑	/Common/script	html

Edit Raise Event on Tag Rule

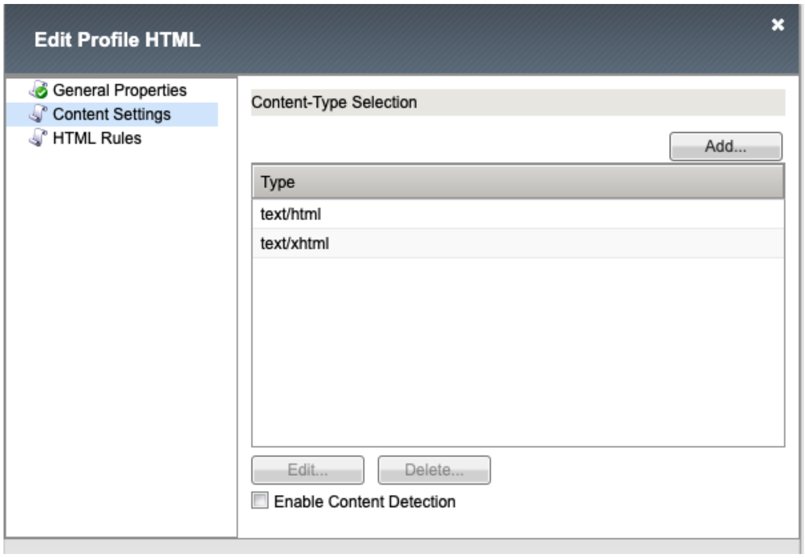
Match Tag Name*: body

Match Attribute Name :

Match Attribute Value :

Under.Local Traffic/Profiles/Content/HTML

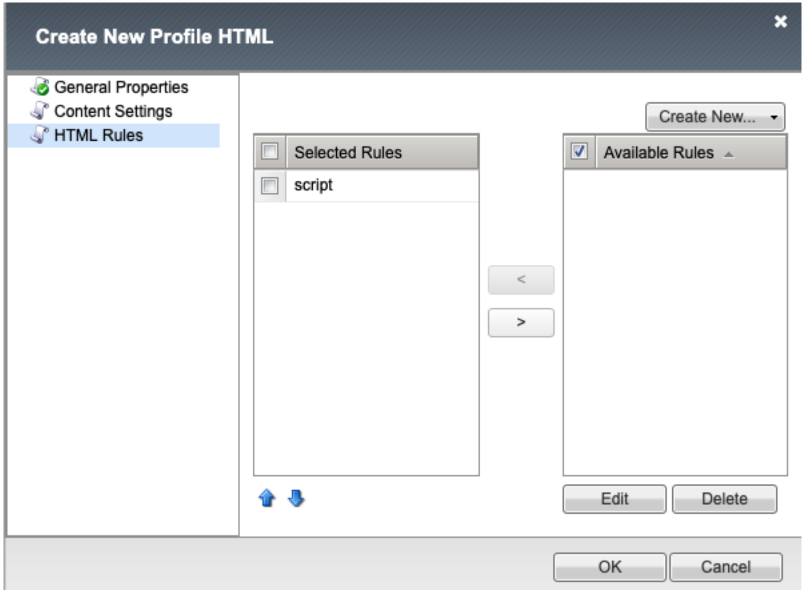
Select Create Profile
Provide a Profile Name
Under Cotent Settings… add a “Content Type Selection” of
“text/html” and
“text/xhtml”



Type
text/html
text/xhtml

□ Enable Content Detection

Under html rules associate the “script” rule that was created above.



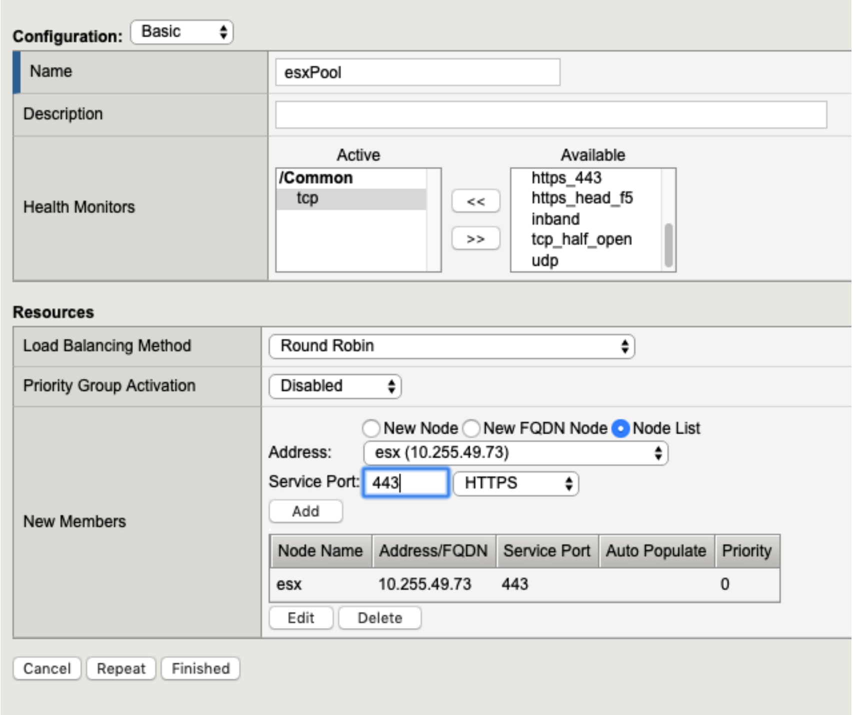
□ Selected Rules
□ script

☑ Available Rules

4) Create a pool for ESXi.

N.B. The pool will be associated with the virtual server for ESXI

Under Local Traffic/Pools/Pool List click “Create”
Provide a Name for the Pool
Select a monitor.
Add the ESXi front end ip as a node to the pool member – make the service port 443 for SSL/TLS.
Click “Finished”



Configuration: Basic

Name	esxPool
Description	
Health Monitors	Active: /Common tcp Available: https_443 https_head_f5 inband tcp_half_open udp

Resources

Load Balancing Method	Round Robin
Priority Group Activation	Disabled
New Members	○ New Node ○ New FQDN Node ● Node List Address: esx (10.255.49.73) Service Port: 443 HTTPS

Node Name	Address/FQDN	Service Port	Auto Populate	Priority
esx	10.255.49.73	443		0

N.B. At this point check that the pool is marked “Available.. “ .. a green circle this will be an indication that the monitor is succeeding and able to make a connection.. the connection type will depend upon the monitor selected.

5) Add the ESXi iRule.

Note: There are a couple of places that require customization with this iRule.

a) Domain for the username.. note that the Active Directory Domain has been appended. Note that with ESXi if you do not set your particular domain as the “Default domain” then the user must append their domain at then end of their user name. For example bob.user@afspc.local. Just also note that users will be logging in most likely with smartcards but this is an internal configuration change that will be customized depending upon your particular domain.

set username [concat [ACCESS::session data get session.logon.last.username]@afspc.local]

b) Redirect in when HTTP_RESPONSE{} event. This will need to be customized for your particular domain. Also the iRule could be modified to add a number of retries in order to limit the possibility of an infinite loop.

```
# Needs an HTML profile and an HTML rule looking for tag "body"
#
# ltm profile html html { app-service none content-selection { text/html text/xhtml } rules {
script } }
# ltm html-rule tag-raise-event script { match { tag-name body } }
# ltm virtual iDRAC-ext { destination 172.16.1.12:https ip-protocol tcp mask 255.255.255.255
pool iDrac profiles { DRAC { } html { } http { } pua_webtop-clientssl { context clientside } rba { }
serverssl { context serverside } tcp { } websso { } } rules { iDracRule } source 0.0.0.0/0 source-
address-translation { type automap } translate-address enabled translate-port enabled vs-index
13 }
```

```
when HTTP_REQUEST {
 HTML::disable
 if {  [HTTP::uri] contains "/websso/SAML2/SSO/vsphere.local" } {
 HTML::enable
 log local0. "HIT LOGIN"
 set workaround 1
 } elseif { [info exists workaround] } {
 unset workaround
 }
}

when HTML_TAG_MATCHED {
 log local0. "at HTML_TAG_MATCHED: [HTML::tag name]"
 if { [info exists workaround] } {
   switch [HTML::tag name] {
     "body" {
       log local0. "at body..."


       set username [concat [ACCESS::session data get session.logon.last.username]@afspc.local]
       set password [ACCESS::session data get session.custom.ephemeral.last.password_sso]
     log local0. $username



     set newstring "<script>
var checkExist = setInterval(function() {
  if (document.body.contains(document.getElementById(\"username\"))) {
    clearInterval(checkExist);



          var un = document.getElementById(\"username\")
          un.focus();
          un.value = \"$username\";

          var ev = document.createEvent('Event');
    ev.initEvent('input', true, false);
    un.dispatchEvent(ev);

          var pw = document.getElementById(\"password\")
          pw.focus();
          pw.value = \"$password\";

          var ev = document.createEvent('Event');
    ev.initEvent('input', true, false);
    un.dispatchEvent(ev);

          var lb = document.getElementById(\"submit\");
          lb.focus();
          lb.click();


  }
}, 4000); // check every 1000ms
</script>"





     HTML::tag append $newstring
     unset workaround
```

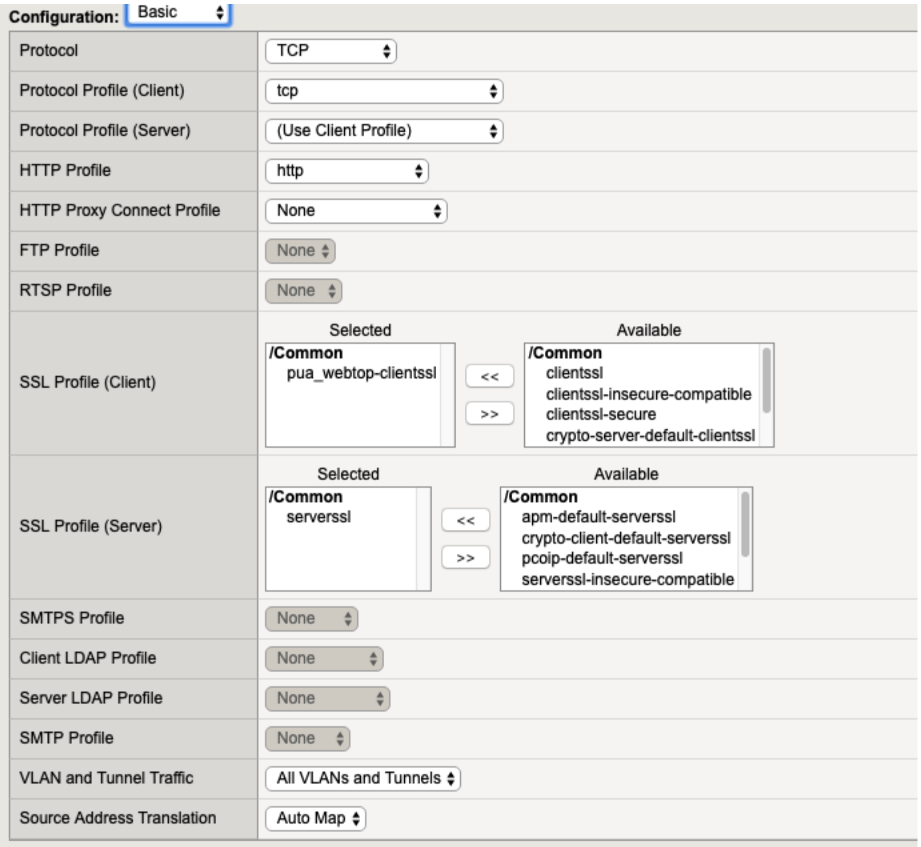
```
        HTML::disable
      }
    }
  }
}


when HTTP_RESPONSE {
   if { ([HTTP::status] starts_with "4") || ([HTTP::status] starts_with "5")} {

          HTTP::redirect "https://gratz-vcenter-6.5.labs.wwtatc.local/ui/#?extensionId=vsphere.core.folder.relatedDatastoresTab&objectId=urn:vmomi:Folder:group-d1:65a04749-387e-44a3-a2db-0087096a756a&navigator=vsphere.core.viTree.hostsAndClustersView"
        }

}
```

6) Create the ESXi VIP.

Under Local Traffic Manager/Virtual Servers Click “Create”

For Source Address:- Your choice.. for instance 0.0.0.0/0
For Destination Address:- This needs to be an IP address.. on the external VLAN.
Service Port: HTTPS

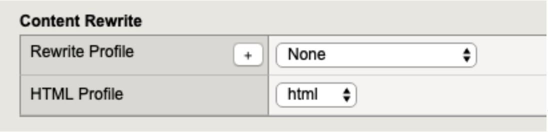
Protocol: TCP
HTTP Profile: http
SSL Profile Client: This needs to be a client SSL profile that is customized for the FQDN for ESXi.
Server SSL: select the “serverssl” profile
Source Address Tranlsation: “Auto Map”



Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	http
HTTP Proxy Connect Profile	None
FTP Profile	None
RTSP Profile	None
SSL Profile (Client)	Selected /Common pua_webtop-clientssl << >> Available /Common clientssl clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl
SSL Profile (Server)	Selected /Common serverssl << >> Available /Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl-insecure-compatible
SMTPS Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
SMTP Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map

Under Content Rewrite Select “html” (Created Previously)

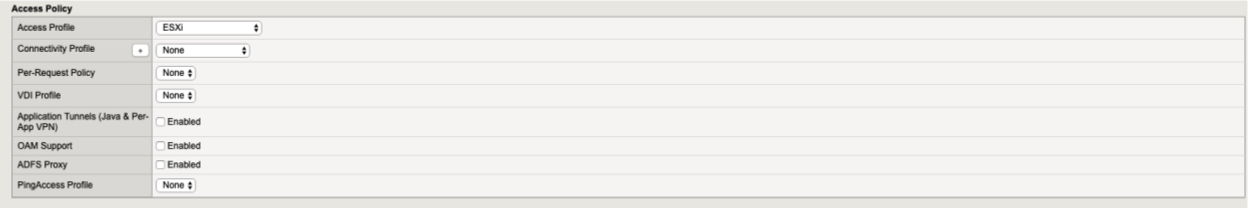


Content Rewrite

Rewrite Profile +	None
HTML Profile	html

]

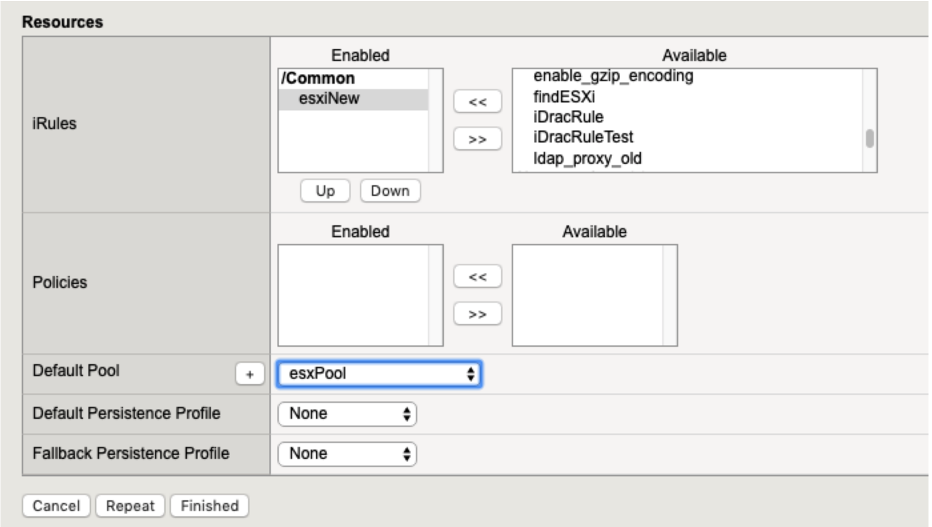
Under Access Policy Select ESXi or whatever you have named your access policy



Access Policy

Access Profile	ESXi
Connectivity Profile +	None
Per-Request Policy	None
VDI Profile	None
Application Tunnels (Java & Per-App VPN)	□ Enabled
OAM Support	□ Enabled
ADFS Proxy	□ Enabled
PingAccess Profile	None

Under Resources
Associate the esxi iRule that was created previously with the VIP
Associate the pool that was created previously wit the VIP
Select “Finished”

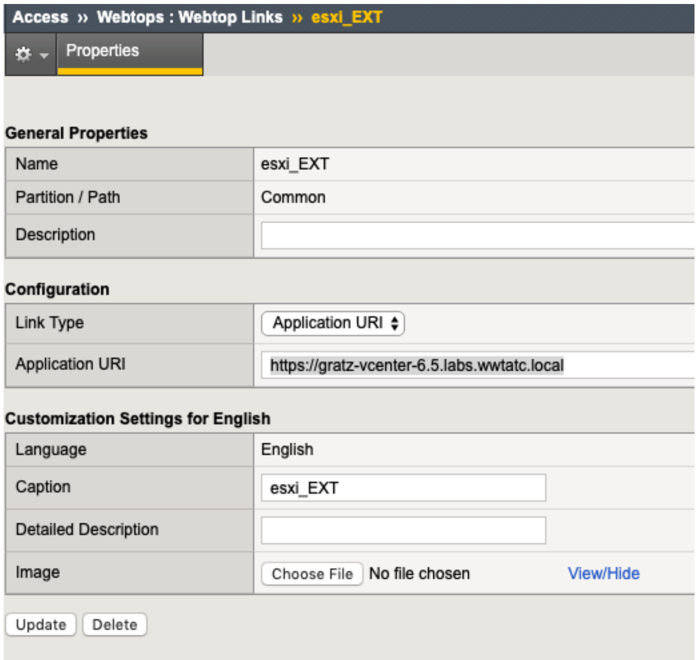


Resources

iRules	Enabled: /Common esxiNew Available: enable_gzip_encoding findESXi iDracRule iDracRuleTest ldap_proxy_old
Policies	Enabled: Available:
Default Pool	esxPool
Default Persistence Profile	None
Fallback Persistence Profile	None

7) Create Portal Access Resource for ESXi

- In the APM menu select Webtops/Webtop Links
  - Click Create
  - Name: Your choice "ESXi" for example
  - Link Type Needs to be Application URI
  - Application URI needs to be the FQDN of the VIP. For example:- https://gratz-vcenter-6.5.labs.wwtatc.local
  - For caption: This will be the name that appears on the webtop.



Access » Webtops : Webtop Links » esxi_EXT

General Properties

Name	esxi_EXT
Partition / Path	Common
Description	

Configuration

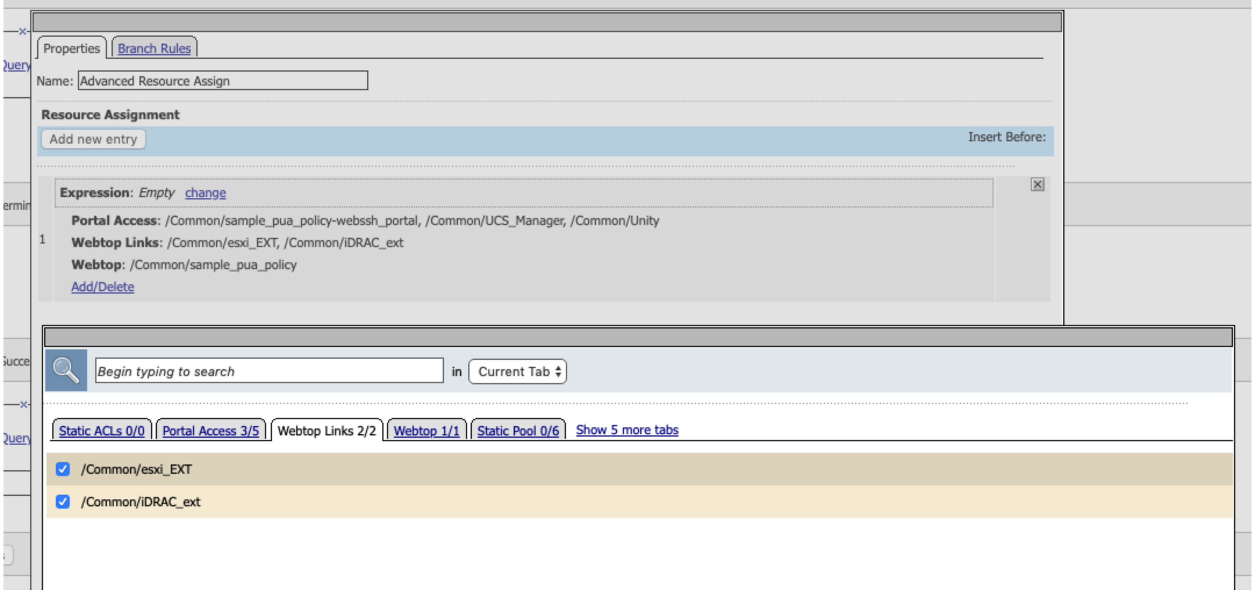
Link Type	Application URI
Application URI	https://gratz-vcenter-6.5.labs.wwtatc.local

Customization Settings for English

Language	English
Caption	esxi_EXT
Detailed Description	
Image	No file chosen

8) You can then associate the ESXi webtop link with the Webtop Policy.

- Click Access/Profiles
- Click "Edit" under Per-Session Policy
- Select the Webtop. This will be associated with an "Advanced Resource Assign Webtop Item"
- Then Select the Add/Delete Button
- Then select the Webtop Links Tab
- Then Select the ESXi webtop link that was created previously.



Name: Advanced Resource Assign

Resource Assignment

Expression: *Empty* change

1 **Portal Access**: /Common/sample_pua_policy-webssh_portal, /Common/UCS_Manager, /Common/Unity
Webtop Links: /Common/esxi_EXT, /Common/iDRAC_ext
Webtop: /Common/sample_pua_policy

☑ /Common/esxi_EXT
☑ /Common/iDRAC_ext